Better bounds on the rate of non-witnesses of Lucas pseudoprimes

David Amirault
Mentor David Corwin
PRIMES conference

May 16, 2015

Starting Small

Theorem (Fermat's Little Theorem)

Let a be an integer and n prime with $n \nmid a$. Then

$$a^{n-1} \equiv 1 \pmod{n}.$$

Starting Small

Theorem (Fermat's Little Theorem)

Let a be an integer and n prime with $n \nmid a$. *Then*

$$a^{n-1} \equiv 1 \pmod{n}.$$

Theorem (Miller-Rabin)

Write $n - 1 = 2^k q$ *with q odd. One of the following is true:*

$$a^q \equiv 1 \pmod{n},$$

or for some m with $0 \leq m < k$,

$$a^{2^m q} \equiv -1 \pmod{n}.$$

Starting Small

Running a Test

Put $1517 - 1 = 2^2 \cdot 379$. Try $a = 2$:

Starting Small

Running a Test

Put $1517 - 1 = 2^2 \cdot 379$. Try $a = 2$:

- $a^{2^0 \cdot 379} \equiv 2^{379} \equiv 923 \not\equiv \pm 1 \pmod{1517}$.
- $a^{2^1 \cdot 379} \equiv 2^{758} \equiv 892 \not\equiv -1 \pmod{1517}$.

Starting Small

Running a Test

Put $1517 - 1 = 2^2 \cdot 379$. Try $a = 2$:

- $a^{2^0 \cdot 379} \equiv 2^{379} \equiv 923 \not\equiv \pm 1 \pmod{1517}$.
- $a^{2^1 \cdot 379} \equiv 2^{758} \equiv 892 \not\equiv -1 \pmod{1517}$.

Thus, 1517 is not prime $(1517 = 37 \cdot 41)$.

Generalizing Integers

Definition

A *quadratic integer* is a solution to an equation of the form

$$x^2 - Px + Q = 0$$

with P, Q integers.

Generalizing Integers

Definition

A *quadratic integer* is a solution to an equation of the form

$$x^2 - Px + Q = 0$$

with P, Q integers.

Theorem

Let $D = P^2 - 4Q$. The set of all quadratic integers in the field $\mathbb{Q}\left[\sqrt{D}\right]$ form a ring, denoted by $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$.

Generalizing Integers

Quadratic Integer Rings

- $D = -4$. The ring of quadratic integers $\mathcal{O}_{\mathbb{Q}[\sqrt{-4}]}$ is the Gaussian integers, $\mathbb{Z}\left[\sqrt{-1}\right]$. Notice $\pm i$ satisfy $x^2 + 1 = 0$, for which $P^2 - 4Q = -4$.

Generalizing Integers

Quadratic Integer Rings

- $D = -4$. The ring of quadratic integers $\mathcal{O}_{\mathbb{Q}[\sqrt{-4}]}$ is the Gaussian integers, $\mathbb{Z}\left[\sqrt{-1}\right]$. Notice $\pm i$ satisfy $x^2 + 1 = 0$, for which $P^2 - 4Q = -4$.
- $D = -5$. Here, $\mathcal{O}_{\mathbb{Q}[\sqrt{-5}]} \cong \mathbb{Z}\left[\sqrt{-5}\right]$.

Generalizing Integers

Quadratic Integer Rings

- $D = -4$. The ring of quadratic integers $\mathcal{O}_{\mathbb{Q}[\sqrt{-4}]}$ is the Gaussian integers, $\mathbb{Z}\left[\sqrt{-1}\right]$. Notice $\pm i$ satisfy $x^2 + 1 = 0$, for which $P^2 - 4Q = -4$.
- $D = -5$. Here, $\mathcal{O}_{\mathbb{Q}[\sqrt{-5}]} \cong \mathbb{Z}\left[\sqrt{-5}\right]$.
- $D = 5$. In this real case, $\mathcal{O}_{\mathbb{Q}[\sqrt{5}]} \cong \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Lucas Primality Test

Theorem

Let P, Q be integers such that $D = P^2 - 4Q \neq 0$. Let τ be the quotient of the two roots of $x^2 - Px + Q$. For n an odd prime not dividing QD, put $n - (D/n) = 2^k q$ with q odd. One of the following is true:

$$\tau^q \equiv 1 \pmod{n},$$

or for some m with $0 \leq m < k$,

$$\tau^{2^m q} \equiv -1 \pmod{n}.$$

Lucas Primality Test

Definition

If n is a composite integer for which $\tau^q \equiv 1 \pmod{n}$ or $\tau^{2^m q} \equiv -1 \pmod{n}$ with $0 \leq m < k$, then we call n a *strong Lucas pseudoprime*, or slpsp, with respect to P and Q.

Lucas Primality Test

Definition

If n is a composite integer for which $\tau^q \equiv 1 \pmod{n}$ or $\tau^{2^m q} \equiv -1 \pmod{n}$ with $0 \leq m < k$, then we call n a *strong Lucas pseudoprime*, or slpsp, with respect to P and Q.

Theorem (Arnault)

Define

$$SL(D,n) = \#\left\{(P,Q)\middle|\begin{array}{ll} 0 \leq P,Q < n, & P^2 - 4Q \equiv D \pmod{n}, \\ \gcd(QD,n) = 1, & n \text{ is slpsp}(P,Q) \end{array}\right\}$$

$SL(D,n) \leq \frac{4}{15}n$ unless $n = 9$ or n is of the form $(2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$, a product of twin primes with q_1 odd.

Better Bounds

Theorem

$SL(D, n) \leq \frac{1}{6}n$ unless one of the following is true:

Better Bounds

Theorem

$SL(D, n) \leq \frac{1}{6}n$ unless one of the following is true:

- $n = 9$ *or* $n = 25$,
- $n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$,
- $n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1+1}q_1 + \varepsilon_2)$,
- $n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1}q_2 + \varepsilon_2)(2^{k_1}q_3 + \varepsilon_3), \quad q_1, q_2, q_3 | q$,

Better Bounds

Theorem

$SL(D, n) \leq \frac{1}{6}n$ unless one of the following is true:

- $n = 9$ *or* $n = 25$,
- $n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$,
- $n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1+1}q_1 + \varepsilon_2)$,
- $n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1}q_2 + \varepsilon_2)(2^{k_1}q_3 + \varepsilon_3), \quad q_1, q_2, q_3 | q$,

where ε_i is determined by the Jacobi symbol (D/p_i) such that p_i is a prime factor of n.

Better Bounds

Suppose we wish to determine that n is prime to a probability of $1 - 2^{-128}$.

Better Bounds

Suppose we wish to determine that n is prime to a probability of $1 - 2^{-128}$.

- $\log_{4/15}(2^{-128}) \approx 67$.
- $\log_{1/6}(2^{-128}) \approx 50$.

Better Bounds

Suppose we wish to determine that n is prime to a probability of $1 - 2^{-128}$.

- $\log_{4/15}(2^{-128}) \approx 67$.
- $\log_{1/6}(2^{-128}) \approx 50$.

17 fewer trials are required using the improved bound.

Solving Exceptions

Quiz!

$\sqrt{961} =$

Solving Exceptions

Quiz!

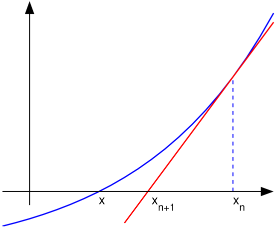
$\sqrt{961} = 31.$

Quiz!

$\sqrt{961} = 31.$

Let x_0 be a guess of a root of the function f. A sequence of better approximations x_n is defined by

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$



Skip Example

Newton's Method

Consider the case $n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$. Does 2627 factor in this form?

Newton's Method

Consider the case $n = (2^{k_1} q_1 - 1)(2^{k_1} q_1 + 1)$. Does 2627 factor in this form?

Write $x = 2^{k_1} q_1$, so $2627 = (x-1)(x+1) = x^2 - 1$ and $x^2 - 2628 = 0$.

Solving Exceptions

Newton's Method

Consider the case $n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$. Does 2627 factor in this form?

Write $x = 2^{k_1}q_1$, so $2627 = (x-1)(x+1) = x^2 - 1$ and $x^2 - 2628 = 0$.

- $x_0 = 40$.
- $x_1 = 40 - \frac{40^2 - 2628}{2 \cdot 40} = 52.85$.
- $x_2 = x_1 - \frac{x_1^2 - 2628}{2x_1} = 51.28782$.
- $x_3 = x_2 - \frac{x_2^2 - 2628}{2x_2} = 51.26403$.

Solving Exceptions

Newton's Method

Consider the case $n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$. Does 2627 factor in this form?

Write $x = 2^{k_1}q_1$, so $2627 = (x-1)(x+1) = x^2 - 1$ and $x^2 - 2628 = 0$.

- $x_0 = 40$.
- $x_1 = 40 - \frac{40^2 - 2628}{2 \cdot 40} = 52.85$.
- $x_2 = x_1 - \frac{x_1^2 - 2628}{2x_1} = 51.28782$.
- $x_3 = x_2 - \frac{x_2^2 - 2628}{2x_2} = 51.26403$.

$\sqrt{2628} = 51.26402$.

Importance

- Primality testing is highly applicable to cryptography.

Importance

- Primality testing is highly applicable to cryptography.
- Many popular cryptosystems, including RSA, require numerous pairs of large prime numbers for key generation.

Importance

- Primality testing is highly applicable to cryptography.
- Many popular cryptosystems, including RSA, require numerous pairs of large prime numbers for key generation.
- Factoring a large semiprime takes more time than multiplying its two prime factors.

Future Research

- The Baillie-PSW primality test combines a Miller-Rabin test using $a = 2$ with a strong Lucas primality test.

Future Research

- The Baillie-PSW primality test combines a Miller-Rabin test using $a = 2$ with a strong Lucas primality test.
- No known composite passes this test.

Future Research

- The Baillie-PSW primality test combines a Miller-Rabin test using $a = 2$ with a strong Lucas primality test.
- No known composite passes this test.
- What must be true of such n?

Acknowledgments

Huge Thanks To:

- David Corwin, my mentor
- Stefan Wehmeier, for suggesting the project
- Dr. Tanya Khovanova, head mentor
- MIT PRIMES
- And of course, my parents for providing transportation and support throughout the project!